AFRIDI & ANGELL
LEGAL CONSULTANTS

Since 1975

inBrief

Proposed New DIFC Data Protection Law

By James Bowden and Kanan Kasuya | 23 July 2019

The DIFC Authority has proposed the enactment of legislation (the **Proposed Law**) to replace its current Data Protection Law, DIFC Law 1 of 2007 (as amended) (the **Current Law**).

The Proposed Law is the subject of Consultation Paper 6 of 2019, which is presently posted on the DIFC website for public comments to be provided by 18 August 2019.

The intention behind the Proposed Law is to align the Current Law with the General Data Protection Regulation (**GDPR**), to reflect the latest technology, privacy and security law developments, and adapt the same to the unique requirements of the DIFC. As GDPR has international application and has become the de facto global standard for data privacy, the Proposed Law is expected to provide consistency and familiarity for businesses in the DIFC that operate on an international scale.

Some noteworthy aspects of the Proposed Law are as follows:

1. Data Subject Rights. In addition to the right to access, rectify and erase personal data and the right to object to Processing which exist under the Current Law, there are new rights introduced in the Proposed Law that are as follows:
    - right to withdraw consent to processing of personal data (**Processing**);
    - right to the restriction of Processing;
    - right to know the recipients of the personal data;
    - right to data portability (*i.e.*, right of a Data Subject to receive its personal data from a Controller in a structured, commonly used and machine-readable format);
    - right to not be subject to automated decision making (including profiling) which produces legal effects concerning, or significantly affects, the Data Subject. Examples of automated decision making include online credit applications and online recruitment tools; and

The Authors

James Bowden
Partner
jbowden@afridi-angell.com
Tel: +971 4 330 3900

James heads the data privacy and cyber security practice at Afridi & Angell. He advises companies in the TMT sector on industry specific regulatory compliance as well as on general corporate and commercial matters. Prior to joining Afridi & Angell, James gained in-depth technology outsourcing experience while working as in-house counsel with one of Canada's leading technology companies. He is a member of the Ontario Bar.

Kanan Kasuya
Associate
kanan@afridi-angell.com
Tel: +971 4 330 3900

Kanan's practice focuses on corporate and commercial matters. She advises clients on general corporate and commercial matters, such as the establishment, structuring and winding down of businesses in the UAE. Kanan joined Afridi & Angell in 2014. She is a member of the Quebec Bar Association.

- right to non-discrimination against a Data Subject for exercising any of the Data Subject rights.

Controllers must make available a minimum of two methods (*e.g.*, by phone, email or online form) by which the Data Subject can contact the Controller to exercise any of the Data Subject rights. Such methods should not be onerous.

2. Apportionment of liability between Controllers and Processors. The Proposed Law (like the Current Law) stipulates that if a Data Subject suffers material or non-material damage by reason of any contravention of the Proposed Law, it will be entitled to compensation.

   Unlike the Current Law, the Proposed Law stipulates when the Controller and the Processor are held liable for the damages caused.

   - A Controller involved in Processing which infringes the Proposed Law shall be liable for damages caused.
   - Processors will be liable where it has not complied with the obligations specifically directed to Processors or where it has acted outside or contrary to the lawful instructions of the Controller.
   - Where multiple Controller(s) or Processor(s) are involved in the Processing and where each is responsible for any damage caused by the Processing, each shall be held jointly and severally liable for the entire damage.

3. Information to be provided to Data Subjects. The Proposed Law has increased the number of items of information to be submitted to the Data Subjects when personal data is collected. The information that must also be provided to the Data Subjects includes (among others):

   - contact details of the Data Protection Officer (if applicable);
   - reference to the appropriate safeguards in the event personal data is transferred to a third country or international organisation;
   - the existence of the Data Subject's right to withdraw consent to the Processing;
   - clarification of the legitimate interest or compliance obligations (for which the personal data is being collected);
   - recipients of the personal data; and
   - any other information to guarantee fair and transparent Processing vis-à-vis the Data Subject, which include (among others):
     - the period of which the personal data will be stored;
     - existence of the other Data Subject rights (set out in point 1 above) as well as the right to lodge a complaint with the Commissioner of Data Protection (the **Commissioner**); and
     - whether Processing will restrict or prevent the Data Subject from exercising any of the Data Subject rights.

   The Proposed Law also specifies that the information must be provided to the Data Subject in writing, including where appropriate by electronic means.

4. Consent to Processing. Controllers must be mindful of the requirements in the Proposed Law to ensure that consent to Processing has been obtained from the Data Subject. Consent under the Proposed Law means clear and unambiguous consent after clear disclosure of every purpose for which the personal data will be collected, processed and used.

5. Requirements for Legitimate and Lawful Processing. The Proposed Law continues the Current Law's requirement for Legitimate Processing (now re-phrased as "Legitimate and Lawful" Processing under the Proposed Law). Personal data must still be processed fairly and transparently vis-à-vis the Data Subject, be limited to the purpose for which it is collected, and must also be accurate (requiring that it be updated via erasure or rectification without undue delay, where necessary).

   The Proposed Law additionally requires that:

   - it would not suffice that Controllers are processing personal data in accordance with the Proposed Law; Controllers would also need to demonstrate such compliance (including to the Commissioner); and
   - personal data must now be kept secure and protected against unauthorised or unlawful Processing and against loss, destruction or damage using appropriate technical or organisational measures.

6. Legitimate Interests. "Legitimate interest" remains one of the grounds under which personal data can be collected. "Legitimate Interests" continue to remain undefined; however, the Proposed Law does introduce two situations which are considered as a "legitimate interest":

   - transferring personal data within a group of undertakings for internal administrative purposes; and
   - processing personal data as strictly necessary and proportionate to ensure network and information security, and to prevent fraud.

   The Proposed Law also introduces restrictions on the use of "legitimate interests" as grounds for Processing. Public authorities cannot rely on such grounds to collect personal data. Furthermore, Controllers who wish to rely on this basis must conduct a careful assessment as to whether a Data Subject can reasonably expect at the time and context to the collection of personal data.

7. Organisational measures to be put in place for DIFC entities. Certain documents and measures would need to be put in place by DIFC entities:

   - technical and organisational measures that ensure personal data is processed in accordance with the Proposed Law and protect the Data Subject's personal data;
   - a written data protection policy proportionate to the processing activities;
   - a policy and process for securely and permanently deleting personal data;
   - a written record in electronic format of the Processing activities; and
   - a written contract in compliance with the Proposed Law (i) between a Controller and a Processor, (ii) between Controllers, and (iii) between a Processor and a sub-Processor. If Processing activity is commenced without such agreement, they would be in breach under the Proposed Law.

   In addition, a DIFC entity transferring personal data to a jurisdiction that lacks an adequate level of protection must take appropriate safeguards. For a discussion of these appropriate safeguards, *see* point 10, below.

8. High Risk Processing Activities. The Proposed Law introduces the concept of "High Risk Processing Activities," which is Processing where one or more of the following applies:

   - new technologies are being deployed which may increase the risk to Data Subjects or render it more difficult for Data Subjects to exercise their rights; or
   - a considerable amount of personal data will be Processed where such Processing is likely to result in a high risk to the Data Subject (on account of the sensitivity of the Personal Data); or

- the Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons (such as profiling), on which decisions are based to produce legal effects on, or significantly affect, the natural person; or
- a non-trivial amount of Special Categories of Personal Data (currently called "Sensitive Personal Data" under the Current Law) is to be Processed.

There are additional obligations that arise for DIFC entities carrying on such activities. These include (among others):

- the appointment of a Data Protection Officer (to assist the Controller and Processor in monitoring the compliance with the Proposed Law); and
- submission of assessments to the Commissioner (namely the Annual Assessment and Data Protection Impact Assessments).

9. Cessation of Processing. The Proposed Law introduces rules on when the Controller must cease the Processing and how personal data must be handled thenceforth.

   Where the basis for Processing ceases to exist or the Controller is required to cease Processing via the exercise of Data Subject rights, the Controller is required to ensure that personal data is securely and permanently deleted, or where this is not possible, archived in a manner such that the data is "put beyond further use." The exception to this rule is where such personal data is necessary for the establishment or defense of legal claims, or to be retained in accordance with applicable laws.

   "Put beyond further use" means that:

   - the Controller must not use the personal data to inform any decision in relation to the Data Subject or in a manner that affects the Data Subject in any way;
   - no party (other than the Controller) has access to the personal data;
   - personal data is protected by appropriate technical and organisational security; and
   - the Controller has in place a strategy for the permanent deletion of personal data, if or when this becomes possible.

10. Transferring personal data to a jurisdiction lacking an adequate level of protection. Unlike in the Current Law, the Commissioner no longer grants a permit or written authorisation to transfer personal data to such jurisdiction. The Proposed Law provides an updated list of conditions, one of which must be satisfied in order to transfer personal data to such jurisdiction:

    - appropriate safeguards must be put in place, which must be in one of the following forms (among others):
      - a code of conduct (approved by the Commissioner) together with binding enforceable commitments of the Controller to apply the appropriate safeguards;
      - a certification mechanism (approved by the Commissioner) together with binding enforceable commitments of the Controller to apply the appropriate safeguards;
      - a legally binding and enforceable instrument;
      - data protection procedures and policies applicable to Group entities, (referred to "Binding Corporate Rules" in the Proposed Law), which may be approved by the Commissioner (but is not mandatory).
    - one of the specific derogations listed in the Proposed Law apply. Such derogations are substantially similar to the transfer conditions set out in the Current Law. This includes (among others) the

transfer is necessary for the performance of a contract or public interest, or that the Data Subject consented to the transfer.

- the transfer satisfies the conditions of "limited circumstances," which is that it is a one-time transfer that concerns only a limited number of Data Subjects, is necessary on the grounds of legitimate interests, and where the Controller has provided suitable safeguards with respect to the protection of personal data. In this situation, the Controller must inform the Commissioner of this transfer.

11. Transferring personal data to a governmental authority outside of DIFC. The Proposed Law introduces guidelines that must be followed in order for the Controllers to disclose and transfer personal data, outside the DIFC, to a governmental authority (the **Requesting Authority**). Controllers must:

    - exercise reasonable caution and diligence to determine the validity and proportionality of the request for personal data;
    - ensure that any disclosure of personal data is made solely for the purpose of meeting the objectives identified;
    - assess the impact of the proposed transfer in light of the potential risks to the Data Subject's rights;
    - implement measures to minimize such risks; and
    - where possible, obtain appropriate and written assurances from the Requesting Authority that it will respect the rights and freedoms of the Data Subjects.

    Failing any of the above, the Controller should not disclose or transfer personal data to the Requesting Authority.

12. Rectification and erasure notification. Controllers must notify each recipient to whom the personal data is disclosed when personal data is rectified, erased or subject to restricted processing.

13. Personal Data Breach. This is a new feature in the Proposed Law. If there is a Personal Data Breach that compromises a Data Subject's confidentiality, security or privacy, the Controller must notify the breach to the Commissioner. When the Personal Data Breach is likely to result in high risk to the Data Subject's confidentiality, security or privacy, the Controller must also communicate the Personal Data Breach to the Data Subjects. ■